DIR Cybersecurity Insight Newsletter

February FY2015 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV

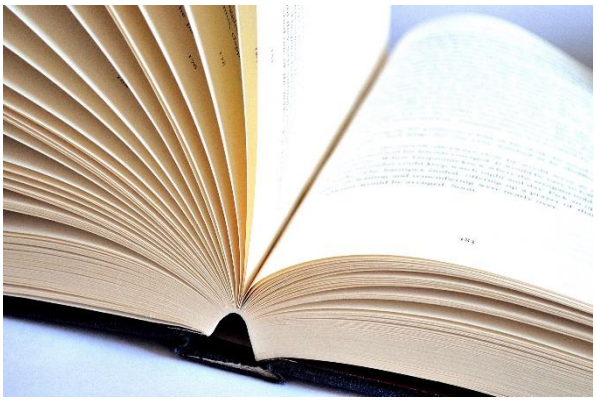
Roses are red
Violets are blue
Cybersecurity needs all of you!

Contents

Cybersecurity - A Love Story

Most of us in the information security field have *'fallen'* or *'jumped'* into this career path. Not many of us set out from a young age to go into information security – but it happened, and for better or worse it becomes a passion.

There are so many facets to information security that it is easy to find something that attracts you to the career path. Whether it's focusing on shoring up your infrastructure defenses, educating your user population, investigating incidents, or playing with the newest tools, cybersecurity has something for everyone.



As many agencies build their security programs, information security officers (ISOs) are discovering the challenge of a shallow workforce. Cybersecurity is not necessarily a career path that one would choose in high school or college. So how can we spread the security love? How do we recruit or usher in a new generation of information security professionals?

This is not only a state issue, but a national issue. This year, the Center for Internet Security (CIS) Education and Awareness Committee is focusing efforts to attract more people to the cybersecurity field. By focusing on educating our youth and working with college students, the CIS hopes to raise interest in this ever-changing career field.

From the state perspective, Texas is working to expand the job classifications for cybersecurity professionals to more clearly define a career path for young professionals. In addition, ISOs are beginning to look outside of the box at individuals with skills that can be applied to information security.

For example, a person with communication and marketing skills may have a knack for explaining complicated issues to management or users in the appropriate manner. A person with teaching experience can bring depth and true substance to an education and awareness program. A veteran employee with detailed knowledge of an agency's infrastructure or applications can work with colleagues to build security into networks and Software Development Life Cycles (SDLCs).

Thinking outside of the box and hiring the unexpected security professional can lead to many positive outcomes, not the least of which could be a new cybersecurity love story.

YOUR ARTICLE HERE!

We want you as a contributor!!!

Send us your article and spread the knowledge. Send your article submissions to DIRSecurity@dir.texas.gov

Program Updates

Texas InfoSec Academy

Since its inception in 2014, enrollment in the InfoSec Academy continues to grow. ISOs are taking both soft skills courses and pre-requisite courses. This spring, a Texas Security Policy & Assurance course will be offered.

Below are some commonly asked questions regarding the InfoSec Academy.

Q: Who is eligible to take InfoSec Academy courses?

A: CISOs and ISOs from state agencies and institutions of higher education are eligible.

Q: Can additional staff enroll in courses?

A: If the CISO/ISO does not intend to take any courses, they may appoint someone else on their staff to participate in their place. If additional people in the agency are interested in taking courses, they can be added to our waiting list.

Q: Do I have to take a soft skills course and the Texas Security Policy and Assurance course before I can take the Certified Security Sentinel or the Certified Vulnerability Assessor course?

A: No, you may enroll in any of these courses without having taken a soft skills course or the Texas Security Policy & Assurance course. However, you cannot enroll in any of the certification prep courses (which will be available at a later date) until you have taken the fundamental courses and the foundational course.

Q: When will the Texas Security Policy & Assurance course be available?

A: DIR expects to begin offering this course in April in an instructor-led classroom environment. A schedule of dates the course will be offered will be released soon. The course will also be available as an online course this summer.

Q: Are continuing education units (CEU) available for Texas InfoSec Academy courses?

A: Yes, after successfully passing the course exams, CEU certificates are available for the Mile2 security courses. You may request one by sending an email to infosecacademy@dir.texas.gov. In the future these may be available from your Mile2 account or within the LMS.

Click here for more information about the InfoSec Academy course tracks.
InfoSec Academy login:
https://infosecacademy.dir.texas.gov/
If you have any questions about the Texas InfoSec Academy, email infosecacademy@dir.texas.gov or call Michele Elledge at 512-475-0419.

Network Security Operations Center (NSOC) Updates

Prompt communication and intelligence sharing along with proper analysis and tools can quicken response time, prevent attacks, and improve overall network security. This was proven at the DIR NSOC in January 2015.

On January 16, the Multi-State Information Sharing and Analysis Center (MS-ISAC) sent an alert stating the DYRE Banking Trojan had recently modified its attack approach to avoid detection and increase the likelihood of infection. This alert also contained information such as IP addresses and domain names considered to be Indicators of Compromise (IOC).

The DIR NSOC immediately went to work analyzing the new information received from MS-ISAC and added the IOC IP addresses and domain names to the intrusion prevention system (IPS) blacklist; this protects the network from future attack attempts.

Next, the DIR NSOC utilized Security Onion – one of the several security tools in use at the NSOC – to research connection logs for previous traffic to the IOC IP addresses and domain names. The NSOC did find evidence of connections to these suspicious IPs, although many of these attempts were just DNS record look-ups. The focus of the investigation was on any connection attempts prior to the new blacklist going into effect. This allowed the NSOC to determine whether an infection had already occurred.

Timely intelligence sharing and appropriate analysis can help to set the proper course of action to take for a potential attack, which includes blocking, monitoring, or alerting DIR customers. Being able to act properly and quickly according to the threat is another key to proper protection and mitigation.

Using appropriate tools (i.e., Security Onion) is critically important to any network infrastructure. Each month the NSOC hosts Statewide Security Operations (SSO) meetings to discuss infrastructure tools. These meetings are a forum to share benefits and challenges of tool use, along with any implementation issues. In 2014, Joe Poole provided in-depth training on Security Onion during these meetings.

If you have any questions regarding NSOC communication and alerts, contact Jeremy Wilson. If you have any questions on Security Onion, contact Joe Poole.

Jeremy A. Wilson
DIR Security Operations Center Manager

Information Security Officer Spotlight

Ken Palmquist, CISSP, Certified Business Continuity Professional, Master Continuity Planner (FEMA), Department of Information Resources

What is your professional history?
I have been in the computer industry for 40 years

How did you come to the security field?
I started working with Medical clinics to assist them in their HIPPA compliance in 2001.

Tell us how information security has changed since you started in your role.
Internet has really complicated things.

What is one of the most challenging areas for you?
Most challenging thing; getting people to take the annual security awareness training.

How did you learn about DIR?
I was brought in as a contractor in 2007 for the migration from Damo (Email) to Exchange and outlook. Then again in 2008 for the migration from Novell to Windows.

What do you like best of your job?
It is *diverse and challenging*

What other career would you have liked to pursue?
Electrical engineer

Where did you grow up?
Dallas and Waco, Texas

Do you have family in Austin?
I have family in Ft Worth and my Mother and younger sister live on my farm.

What are your hobbies?
Woodworking, Astronomy and building street rods and I guess farming.

People would be surprised to know that you…
Build telescopes

Are you messy or organized?
Organized

Favorite travel spot?
Europe – Germany

Which CD do you have in your car? Or what radio station do you listen to?
91.3 Easy listening out of Killen, Texas

If you could interview one person (dead or alive) who would it be?
John Wayne

If you had to eat one meal, every day for the rest of your life, what would it be?
Hamburger

Least favorite food?
Turnip Greens

Describe what you were like at age 10
Boy Scout, messing around with my chemistry lab and building model rockets that fly.

What would be your advice for a new security professional?
Get in there and learn all you can.

Insight from our former Texas CISO

Brian Engle
Former CISO, State of Texas

When you receive this newsletter I will no longer be in the role of State of Texas CISO. As a last article for the Insights newsletter, there are a million topics that I considered writing about, but I would like to share with you my perspectives on community. Over the past three years, I have learned a lot from each of you about the sense of community, serving together to protect information and information resources for our citizens and our great state.

I am thankful that the community of state security professionals was open and gracious to include me when I came to the Health and Human Services Commission over three years ago and continuing through the time here at the Department of Information Resources. Through several great leaders within the state's agencies, I was able to quickly meet and get to know many information security officers, and the comradery helped me gain an understanding for the issues and constraints that agencies were facing.

The need for collaboration within the information security community is continually demonstrated as we see the industry grow and evolve. Scarcity of resources and the survival instincts of the security professional that often is a department of one creates a strange sense of isolationism with a need to seek the company of others. Certainly collaboration can occur without the support of a community. Mentors, colleagues, and personal relationships used in conjunction with ongoing professional development all serve to help us progress as experts. But I believe that progress occurs at a higher rate for all when community can be leveraged to expand upon collaboration opportunities.

Collaboration does not come without obstacles. Trust is instilled through honest and ongoing communication and is typically limited to relationships where common ground can be established. Face to face engagement certainly helps, and history between the individuals also creates an environment for trust. Communication can be difficult as we all work tirelessly to accomplish all of the priority items before us. Work life balance, whatever that is, also forces you to make decisions about where you invest your time.

So why all this talk about community and collaboration? As I consider the challenges and the scope of my new role, my highest priority is to establish a cybersecurity team to be my eyes and ears to the customers' needs to ensure confidence and the highest quality security services.

I envision a cybersecurity team that obtains and shares critical information and intelligence and establishes best practices for identifying cybersecurity threats and risks while preserving the integrity of information and technology resources.

Our cybersecurity team will provide round-the-clock services to detect, identify, and halt suspicious and malicious activities and to respond quickly and effectively to limit damage and theft. Response will be compliance with an established plan with a clear goal for quick reaction to incidents with the focus on full and quick recovery.

Finally, I envision a cybersecurity team that works together in the interest of survival and to forge trusted relationships and partners for a common goal.
I want to encourage each of you to continue to participate in this community of Texas security practitioners and get involved in areas that can help you most or where you can help someone else. As a now former and recovering CISO, I intend to continue to contribute to the community through the Texas CISO Council, InfraGard, ISSA, ISACA, OWASP, and anywhere that DIR will continue to permit me to help. As a citizen of this great state and country, I'm counting on each of you with trust and great respect for all that you do.

Good luck and God bless!

Brian Engle

Events

Training and Conferences Around the State

Monthly Security Program Webinar
Identity and Security Intelligence: Bringing them together with SIEM
Date: Tuesday, March 10th, 2015
Time: 2:00 pm CDT
https://attendee.gotowebinar.com/register/8803618443472383234

ISF Information Security Forum for Texas Government **2015**

Date: Wednesday-Thursday, May 20-21, 2015 |
Time: 8:00 - 4:30
Place: Palmer Events Center
900 Barton Springs Road
Austin, Texas 78704

2015 Save the Dates

- BSides Austin: March 12 – 13 http://bsidestexas.blogspot.com/p/austin-2013.html
- BSides San Antonio: May 10 http://bsidestexas.blogspot.com/p/san-antonio-april-2013.html
- ISO 27001 summit: May 13-14
- Blackhat USA: August 1 – 6 https://www.blackhat.com/us-15/
- BSides Las Vegas: August 5 – 6
- Defcon 23: August 6 – 9 https://www.defcon.org/
- LASCON 2015: October 19 – 22
- Dallas Secure World: October 28-29, 2015

Feedback, comments, stories, etc.
DIRSecurity@dir.texas.gov

Office of the CHIEF INFORMATION SECURITY OFFICER State of Texas